UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/730,926	12/10/2003	Jean-Marc Robert	ALC 3106	6727

7590 12/28/2006

KRAMER & AMADO, P.C.
Suite 240
1725 Duke Street
Alexandria, VA 22314

EXAMINER	
YALEW, FIKREMARIAM A	
ART UNIT	**PAPER NUMBER**
2136	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	12/28/2006	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/730,926	ROBERT, JEAN-MARC	
	Examiner	Art Unit	
	Fikremariam Yalew	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 December 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *05/18/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-22 have been examined.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claims 1 and 13 are recited under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

4. Claims 1 and 13 are directed to a method of tracking-back a malicious data packet in a connection oriented communication network. The examiner respectfully asserts that the claimed subject matter does not fall within the statutory classes listed in 35 USC 101.The claimed steps do not result in a tangible result. (i.e., it just stores non functional data. On the preamble the applicant intend to do a method of tracking-back a malicious data packet but that on dependent claim 2,3). Claims 1,13 are rejected as being directed to an abstract idea (i.e., producing non-tangible result).

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1,4-8,10-13 are rejected under 35 U.S.C. 102(e) as being anticipated by Milliken (US Patent 6,978,223 B2).

7. As per claim 1: Milliken discloses a method of tracking-back a malicious data packet in a connection-oriented communication network, comprising the steps of: a) for a given time window (Time Period), computing a unique flow identifier (FlowId) for each packet of a given flow seen by a router interface (Incoming Link) at a network node (See Fig 8 steps 805,505,510, 515 and col 3 lines 11-21); b) inserting said FlowId into a data structure associated to said Time Period and said Incoming Link, available at said network node (See Fig 8 steps 805,505,510,515); c) storing said data structure in a searchable repository(Fig 4 step 405); and d) repeating steps a) to c) for a next Time Period and for each Incoming link at said network node(See Fig 10).

8. As per claim 4: Milliken discloses the method wherein step a) is based on flow definition adopted for said network (See Fig 1 and col 4 lines 17-38).

9. As per claim 5: Milliken discloses the method wherein step a) comprises applying a specified function to one or more header fields of each packet received in said flow (See Fig 5 steps 505,510,515).

10. As per claim 6: Milliken discloses the method wherein step a) comprises applying a specified function to one or more header fields of each packet received in said flow and an incoming interface identification parameter (See Fig 10 step 1015 and Fig 8 step 805).

11. As per claim 7: Milliken discloses the method wherein step a) comprises applying a specified function to one or more characteristics of each packet (See Fig 5 steps 505,510,515 and col 3 lines 11-20).

12. As per claim 8: Milliken discloses the method wherein step a) comprises applying a specified function to one or more characteristics of each packet received in said flow and an incoming interface identification parameter (See Fig 5 steps 505,510,515 and col 3 lines 11-20).

13. As per claim 10: Milliken discloses the method wherein said searchable repository is maintained for each router interface at said network node (See Fig 7 step 705 and col 3 lines 38-40).

14. As per claim 11: Milliken discloses the method wherein said searchable repository stores all said data structures for all router interfaces at said network node (See Fig 10 steps 1010,1015).

15. As per claim 12: Milliken discloses the method wherein said searchable database is a centralized searchable repository maintained for said network (See Fig 4 and col 6 lines 11-37).

16. As per claim 13: Milliken discloses a method of tracking-back a malicious data packet in a connection-oriented communication network, comprising the steps of: a) for a given time window (Time Period), computing a unique flow identifier (FlowId) for each packet of a given flow seen by a router interface (Incoming Link) at a network node based on a flow characterization parameter obtained from management system (See Fig 8 steps 805,505,510, 515 and col 3 lines 11-21); b) inserting said FlowId into a data structure associated to said Time Period and said Incoming Link, available at said network node (See Fig 8 steps 805,505,510,515); c) storing said data structure in a searchable repository(Fig 4 step 405); and d) repeating steps a) to c) for a next Time Period and for each Incoming link at said network node(See Fig 10).

Claim Rejections - 35 USC § 103

17. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

18. Claims 2-3,9,14-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over by Milliken (US Patent 6,978,223 B2) in view of Snoeren et al (Hash based IP Traceback, 27 Augest 2001).

19. As per claim 2: Mikkiken does not explicitly disclose the method of further comprising: e) determining the time of arrival X of said malicious packet at said network node and computing FlowId for said malicious packet; and f) identifying said Incoming Link for said malicious packet by searching for the FlowId of said malicious packet in all data structures for said network node that cover the time of arrival X.

However Snoeren teaches e) determining the time of arrival X of said malicious packet at said network node and computing FlowId for said malicious packet; and f) identifying said Incoming Link for said malicious packet by searching for the FlowId of said malicious packet in all data structures for said network node that cover the time of arrival X (See pages 1-3 and page 12 the conclusion).

It would have been obvious to one ordinary skill in the art at the time the invention was made to modify the teaching method of Mikkiken to include e) determining the time of arrival X of said malicious packet at said network node and computing FlowId for said malicious packet; and f) identifying said Incoming Link for said malicious packet by searching for the FlowId of said malicious packet in all data structures for said network node that cover the time of arrival X. This modification would have been motivated to do so, as suggested by, (Snoeren page 2) inorder to reduce the memory requirement through the use of Bloom filter.

20. As per claim 3: the combination of Milliken and Snoeren teach further comprising tracing-back hop by hop the source of said single packet from said router, by performing steps e) and f) for each network node along the path of said malicious packet (See page 4 section 3.3).

21. As per claim 9: Milliken teach claim 1 as recited above. Milliken does not explicitly teach the method wherein said data structure is a hash table based on a Bloom filter. However Snoeren teach the combination of Milliken and Snoeren the method wherein said data structure is a hash table based on a Bloom filter (See page 2 first paragraph).

Therefore It would have been obvious to one ordinary skill in the art at the time the invention was made to modify the teaching method of Milliken to include the method wherein said data structure is a hash table based on a Bloom filter. This modification would have been motivated to do so, as suggested by, (Snoeren page 2) inorder to reduce the memory requirement through the use of Bloom filter.

22. As per claim 14: Milliken disclose a system for tracking-back a malicious data packet in a connection-oriented communication, comprising: means for computing a unique flow identifier FlowId for each packet of a flow seen by a router interface (Incoming Link) at a network node over a given period of time (Time Period); means for inserting said FlowId into a data structure associated to said Time Period (See Fig 8 steps 805,505,510, 515), and said Incoming Link available for said network node; a searchable repository for storing said data structure(Fig 4 step 405).

Mikkiken does not explicitly teach a search engine for finding in said searchable repository the Incoming Link for said malicious packet based on a FlowId and a time of arrival X of said malicious packet.

However Snoeren discloses a search engine for finding in said searchable repository the Incoming Link for said malicious packet based on a FlowId and a time of arrival X of said malicious packet (See pages 1-3 and page 12 the conclusion).

Therefore It would have been obvious to one ordinary skill in the art at the time the invention was made to modify the teaching method of Mikkiken to include a search engine for finding in said searchable repository the Incoming Link for said malicious packet based on a FlowId and a time of arrival X of said malicious packet. This modification would have been motivated to do so inorder to enhance the security of the system.

23. As per claim 15: the combination of Milliken and Snoeren teach the system further comprising a flow-based monitoring system for tracking back hop-by-hop the source of said malicious packet (See Snoeren page 4 section 3.3)

24. As per claim 16: the combination of Milliken and Snoeren teach the system wherein one said searchable repository is maintained for each interface at said network node (See Milliken Fig 7 step 705 and col 3 lines 38-40).

25. As per claim 17: the combination of Milliken and Snoeren teach the system of wherein one said searchable repository is maintained for said network node (See Milliken Fig 4 and col 6 lines 11-37).

26. As per claim 18: the combination of Milliken and Snoeren teach the system of wherein said searchable repository is a centralized database maintained for said network (See Milliken Fig 4 and col 6 lines 11-37).

27. As per claim 19: the combination of Milliken and Snoeren teach the system of further comprising a flow based monitoring system for providing a flow characterization parameter to said means for calculating (See Milliken Fig 12 step 1210).

28. As per claim 20: the combination of Milliken and Snoeren teach the system further comprising a flow management system for generating a flow characterization parameter (See Milliken Fig 9 step 915).

29. As per claim 21: the combination of Milliken and Snoeren teach the system of wherein said means for computing is a FlowId calculator for computing said FlowId form one or more of packet header fields, packet characterization parameters and interface identification information (See Milliken Fig 12 steps 1230,1235).

30. As per claim 22: the combination of Milliken and Snoeren teach the system wherein said means for computing is a FlowId calculator for computing said FlowId form packet header information (See Milliken Fig 12 step 1205).

Conclusion

31. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO 892.

32. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fikremariam Yalew whose telephone number is 5712723852. The examiner can normally be reached on 9-5.

33. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser can be reached on 5712724195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Fikremariam Yalew
12/19/2006
FA

Art Unit 2136

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

12/20/06